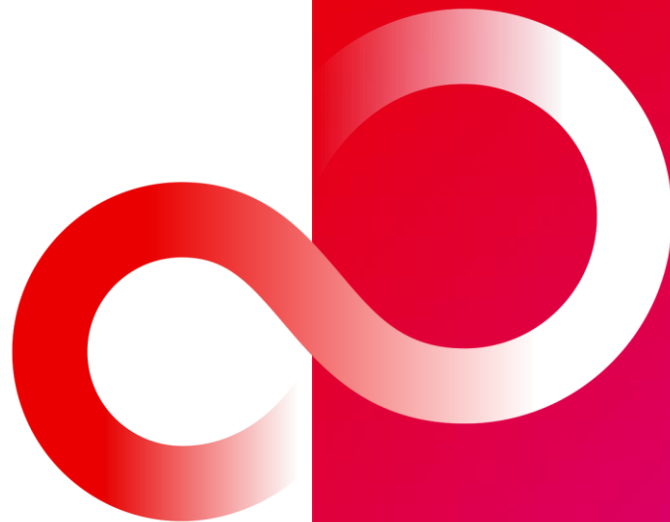


YoctoのSPDXについて

2022/2/4

富士通)安倍昌輝



- はじめに
 - Yoctoとは
 - SPDXとは
- YoctoでSPDXを作成するツールの紹介
 - meta-spdxscanner
 - create-spdx
 - 各ツールのメリット/デメリット
- 各ツールのSPDXを検証と比較
- SPDXの最新状況
 - SPDX DocFest on January 27th
 - 感想

● Yocto Projectとは

- 組み込みLinuxディストリビューションを標準化するために立ち上げられた。
- Linuxを構築するために、BitBakeというビルドツールやOSSパッケージをビルドするためのレシピなどを提供している。

<https://www.yoctoproject.org/>

● SPDXとは

- Software Package Data Exchange (SPDX)
- SPDXは、コンポーネント、ライセンス、著作権などのソフトウェア情報を伝達するためのオープンな標準です。

<https://spdx.dev/>

● 概要

- meta-spdxscannerは、spdxファイルの作成に使用できるYoctoのlayerです。
- <https://git.yoctoproject.org/meta-spdxscanner/>

● 特徴

- SPDX仕様のバージョンは 2.2
- FOSSologyなどのOSSのツールと連携して、ソースコードをスキャンしてライセンスを検出する

● 連携ツール

- FOSSology
- ScanCode Toolkit
- Black Duck

- 出力形式 : tag-value
- 例 : busybox-1.34.1
(FOSSology連携)

```
##-----  
## Creation Information  
##-----  
  
Creator: Tool: fossology-python.bbclass in meta-spdxscanner  
Creator: Person: fossy (y)  
CreatorComment: <text>  
This document was created using license information and a generator from Fossology.  
</text>  
Created: 2021-10-15T08:30:34Z  
LicenseListVersion: 2.6  
  
##-----  
## Package Information  
##-----  
  
PackageName: busybox  
PackageVersion: 1.34.1  
PackageFileName: busybox-1.34.1-r0-patched.tar.gz  
SPDXID: SPDXRef-upload1404  
PackageDownloadLocation: https://busybox.net/downloads/busybox-1.34.1.tar.bz2;name=tarball  
PackageHomePage: https://www.busybox.net  
PackageSummary: <text>Tiny versions of many common UNIX utilities in a single small execut  
PackageVerificationCode: da39a3ee5e6b4b0d3255bfef95601890afd80709  
PackageDescription: <text>busybox version 1.34.1</text>  
PackageComment: <text>
```

● 概要

- OpenEmbedded Coreのlayerに含まれるクラスファイルのひとつ。
- <https://git.openembedded.org/openembedded-core/tree/meta/classes/create-spdx.bbclass>

● 特徴

- SPDX仕様のバージョンは 2.2
- ソースコードをスキャンしない
- Yoctoのrecipeファイルの“LICENSE”項目からライセンス情報を取得する
 - 例 : busybox-1.34.1
LICENSE = "GPLv2 & bzip2-1.0.4"
<http://cgit.openembedded.org/openembedded-core/tree/meta/recipes-core/busybox/busybox.inc?h=honister>
<http://git.openembedded.org/openembedded-core/tree/meta/classes/create-spdx.bbclass#n442>

- 出力形式 : json
- 例 : busybox-1.34.1

```
{
  "SPDXID": "SPDXRef-DOCUMENT",
  "creationInfo": {
    "comment": "This document was created by analyzing packages created during the build.",
    "created": "2021-10-15T04:04:06Z",
    "creators": [
      {
        "Tool": "OpenEmbedded Core create-spdx.bbclass",
        "Organization": "OpenEmbedded ()",
        "Person": "N/A ()",
        "licenseListVersion": "3.14",
        "dataLicense": "CC0-1.0",
        "documentNamespace": "http://spdx.org/spdxdoc/busybox-src-d03ca829-5435-5059-972a-003f25de1edf",
        "externalDocumentRefs": [
          {
            "checksum": {
              "algorithm": "SHA1",
              "checksumValue": "0c88738ad8d827a8e29dedc8c75695c9130187f4"
            },
            "externalDocumentId": "DocumentRef-recipe-busybox",
            "spdxDocument": "http://spdx.org/spdxdoc/recipe-busybox-1dd695ee-b779-5d09-9314-a0c15f2a4031"
          }
        ],
        "files": [
          {
            "SPDXID": "SPDXRef-PackagedFile-busybox-src-1",
            "checksums": [
              {
                "algorithm": "SHA1",
                "checksumValue": "c8a6f275a6a99ba17a7c981b5edd2b2cb48b82a1"
              },
              {
                "algorithm": "SHA256",
                "checksumValue": "9da b4018b1e2b54613ea4142a561b25bb9fa27f8be8015c82c268bbe5135be16"
              }
            ],
            "copyrightText": "NOASSERTION",
            "fileName": "usr/src/debug/busybox/1.34.1-r0/busybox-1.34.1/util-linux/blkid.c",
            "fileTypes": [
              "BINARY"
            ],
            "licenseConcluded": "NOASSERTION",
            "licenseInfoInFiles": [
              "NOASSERTION"
            ]
          },
          {
            "SPDXID": "SPDXRef-PackagedFile-busybox-src-2",
            "checksums": [
              {
                "algorithm": "SHA1",
                "checksumValue": "1382c3dc5473af7c2517edbd7b4a5770c3f7f47e"
              },
              {
                "algorithm": "SHA256",
                "checksumValue": "96f4d793e5cd5c5cd088df05b4ca8c6109abaa87c664e3c9b4aa0b850f20d302"
              }
            ],
            "copyrightText": "NOASSERTION",
            "fileName": "usr/src/debug/busybox/1.34.1-r0/busybox-1.34.1/util-linux/fstrim.c",
            "fileTypes": [
              "BINARY"
            ],
            "licenseConcluded": "NOASSERTION",
            "licenseInfoInFiles": [
              "NOASSERTION"
            ]
          },
          {
            "SPDXID": "SPDXRef-PackagedFile-busybox-src-3",
            "checksums": [
              {
                "algorithm": "SHA1",
                "checksumValue": "2916c208dcb93dc341028cf68c69a50d2f9073c8"
              },
              {
                "algorithm": "SHA256",
                "checksumValue": "29256cf913b3a1f6c050bf9ff2efdece64dc5e002dd62f9db7b0ba3e116f677f"
              }
            ],
            "copyrightText": "NOASSERTION",
            "fileName": "usr/src/debug/busybox/1.34.1-r0/busybox-1.34.1/util-linux/losetup.c",
            "fileTypes": [
              "BINARY"
            ],
            "licenseConcluded": "NOASSERTION",
            "licenseInfoInFiles": [
              "NOASSERTION"
            ]
          },
          {
            "SPDXID": "SPDXRef-PackagedFile-busybox-src-4",
            "checksums": [
              {
                "algorithm": "SHA1",
                "checksumValue": "eb453a574ddb9c715180d01775303437dc8ec75"
              },
              {
                "algorithm": "SHA256",
                "checksumValue": "3d264a3d411ea81771f590dc9f3861854231aba6e40851584d2fc397e31740e0"
              }
            ],
            "copyrightText": "NOASSERTION",
            "fileName": "usr/src/debug/busybox/1.34.1-r0/busybox-1.34.1/util-linux/dmccg.c",
            "fileTypes": [
              "BINARY"
            ],
            "licenseConcluded": "NOASSERTION"
          }
        ]
      }
    ]
  }
}
```

● meta-spdxscanner

メリット

- ソースコードをスキャンしてファイル単位のライセンスが検出可能
- 様々なOSSのツールと連携が可能

デメリット

- 検出したライセンスの精査が必要

● create-spdx

メリット

- 手軽にSPDXファイルを作成可能

デメリット

- ライセンスの精度はrecipeに依存

Yoctoコミュニティとして、recipeの正確性を確保する仕組みづくりが必要

常に最新のソースでライセンスを精査し、recipeの正確性を確保するためにmeta-spdxscannerが活用出来ないかと考える

- SPDXの検証

- SPDX Online Toolを使用してSPDXの形式が正しいか検証
<https://tools.spdx.org/app/validate/>

- meta-spdxscannerの検証結果

- warningが発生

The following warning(s) were raised: [Missing required SPDX version]

- 1行目 SPDXVersionの前に不要な文字が存在するため

b'SPDXVersion: SPDX-2.2

- 削除すると検証は成功する

This SPDX Document is valid.

- create-spdxの検証結果

- warningが発生

- The following warning(s) were raised: [Invalid package declared license: Incompatible type for property member: class org.spdx.library.model.license.AnyLicenseInfo]*

- licenseDeclaredで宣言されたライセンスのタイプに誤りがある

- "licenseDeclared": "GPL-2.0-only AND DocumentRef-recipe-busybox:LicenseRef-bzip2-1.0.4",*

- 削除すると検証は成功する

- This SPDX Document is valid.*

各SPDXの項目を比較

SPDX section	Field	Required	meta-spxscanner	create-spx
6	SPDX Version	Yes	SPDX-2.2	SPDX-2.2
6	Data License	Yes	CC0-1.0	CC0-1.0
6	SPDX Identifier	Yes	SPDXRef-DOCUMENT	SPDXRef-DOCUMENT
6	Document Name	Yes	busybox-1.34.1	http://spdx.org/spdxdoc/busybox-src-d03ca829-5435-5059-972a-003f25de1edf
6	SPDX Document Namespace	Yes	http://916014a1c5a4/repo/SPDX2TV_bu-sybox-1.34.1-r0-patched.tar.gz_1634286632.spdx	http://spdx.org/spdxdoc/recipe-busybox-1dd695ee-b779-5d09-9314-a0c15f2a4031
6	Creator	Yes	Tool: fossology-python.bbclass in meta-spxscanner	Tool: OpenEmbedded Core create-spx.bbclass
6	Created	Yes	2021-10-15T08:30:34Z	2021-10-15T04:04:06Z
7	Package Name	Yes	busybox	busybox-src
7	Package SPDX Identifier	Yes	SPDXRef-upload1404	SPDXRef-Package-busybox-src
7	Package Version	No	1.34.1	1.34.1

各SPDXの項目を比較

7	Package File Name	No	busybox-1.34.1-r0-patched.tar.gz	項目なし
7	Package Download Location	Yes	https://busybox.net/downloads/busybox-1.34.1.tar.bz2;name=tarball	NOASSERTION
7	Files Analyzed	No	項目なし	項目なし
7	Package Home Page	No	https://www.busybox.net	項目なし
7	Concluded License	Yes	NOASSERTION	NOASSERTION
7	Declared License	Yes	NOASSERTION	GPL-2.0-only AND DocumentRef-recipe-busybox:LicenseRef-bzip2-1.0.4
7	Comments on License	No	licenseInfoInFile determined by Scanners: - nomos ("3.11.0".c93921) - monk ("3.11.0".c93921) - ojo ("3.11.0".c93921)	項目なし
7	Copyright Text	Yes	NOASSERTION	NOASSERTION
7	Package Comment	No	ModificationRecord: true PackageLicenseInfoInLicenseFile: LICENSE: GPL-2.0 PackageLicenseInfoInLicenseFile:	項目なし

各SPDXの項目を比較

8	File Name	Yes	busybox-1.34.1-r0-patched.tar.gz/busybox-1.34.1-r0-patched.tar/spdx_temp/busybox-1.34.1/util-linux/blkid.c	usr/src/debug/busybox/1.34.1-r0/busybox-1.34.1/util-linux/blkid.c
8	Concluded License	Yes	NOASSERTION	NOASSERTION
8	License Information in File	Yes	GPL-2.0	NOASSERTION
8	Copyright Text	Yes	Copyright (C) 2008 Denys Vlasenko.	NOASSERTION
10	License Identifier	Conditional	LicenseRef-UnclassifiedLicense	項目なし
10	Extracted Text	Conditional	An unclassified license reference looks like a license (it contains common license terminology) but we don't recognize a specific license.	項目なし
10	License Name	Conditional	UnclassifiedLicense	項目なし
10	License Comment	No	項目なし	項目なし

- SPDX DocFest on January 27th
 - 日本時間 2022年01月28日(金) 00:00 - 04:00 に開催された
 - 目的は、SPDXファイルの作成者や利用者を集め、同じソフトウェア成果物に対するツール出力と理解の違いについて話し合うこと
- 対象ソフトウェア
 - PyYAML (Source and binary)
 - Container version: `automatingcompliance/tooling/spdxdocfest:pyyaml`
 - App-BOM-ination (This is a BOM torture test)
 - Container version: `automatingcompliance/tooling/spdxdocfest:appbomination`

- 参加した組織 or Tool 計 : 13

- Canvass Labs, FOSSology, Kubernetes, metaffekt, meta-spdxscanner, nexB, OpenEmbedded, Philips, REA, SourceAuditor, Synopsys Black Duck, Tern, Zephyr west

- 検証結果の指摘例

- Canvass Labs : App-BOM-inationの解析に失敗している
- SourceAuditor : LicenseInfoFromFiles に複雑なライセンスが含まれている
- Tern : verification valueがない

● 議論のトピックス

- determine if chosen inconsistency is a result of a spec ambiguity/misunderstanding or a tool issue
- Package naming best practices
- Concluded license ...etc.

● 参加した個人的な感想

- 参加の多さに驚いた。また世界的にも注目されている事を改めて認識
- 自分が知らないツールも知る事ができ参加して良かった
- Concludedライセンスをツールが決定できる仕組みが確立して欲しい
- 提供されてツールの出力結果でJSONが増えていた。他のツールとも連携する機会が多くなったと考える。
普及してくる前は各項目が分かり易いTag-value形式が多かったと感じる
- 議論が中心であったため、自身の英語力の低さが身に染みた。。。

Thank you

